

No. 26-1444

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

AMAZON.COM SERVICES, LLC,
Plaintiff-Appellee,

v.

PERPLEXITY AI, INC.,
Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR
SAN FRANCISCO, NORTHERN CALIFORNIA IN
CASE NO. 3:25-CV-09514-MMC
MAXINE M. CHESNEY, DISTRICT JUDGE

**Brief of News/Media Alliance as *Amicus Curiae* in Support of
Plaintiff-Appellee**

Michael S. Elkin
Sean R. Anderson
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166
(212) 294-6700
melkin@winston.com
sranderson@winston.com

Jennifer A. Golinveaux
Thomas J. Kearney
WINSTON & STRAWN LLP
101 California Street, Floor 21
San Francisco, CA 94111
(415) 591-1000
jgolinveaux@winston.com
tkearney@winston.com

Attorneys for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and Ninth Circuit Rule 29-1, News/Media Alliance is a nonprofit organization that has no parent corporation, and no publicly held company owns 10% or more of its stock.

TABLE OF CONTENTS

	Page
STATEMENT OF INTEREST OF <i>AMICUS CURIAE</i>	1
RULE 29(a)(4)(E) CERTIFICATION	2
SUMMARY OF ARGUMENT	3
ARGUMENT	8
I. NEWS ORGANIZATIONS RELY ON THE ABILITY TO EFFECTIVELY MANAGE ACCESS TO THEIR CONTENT TO BE ECONOMICALLY VIABLE IN AN ONLINE ENVIRONMENT.....	8
II. ACCESS IN CONTRAVENTION OF PROHIBITIONS AGAINST AI AGENTS OR “BOTS” VIOLATES THE CFAA.....	12
A. Perplexity’s Conduct Violates the CFAA Because Perplexity Itself Accesses a Protected Website but Lacks Authorization to Do So.....	12
B. The Type of Information Perplexity Obtained from Amazon’s Protected Website Implicates the CFAA.....	15
C. Perplexity’s Continued Access After Amazon Expressly Prohibited It from Accessing Password-Protected Areas of the Website Violated the CFAA	16
D. Bots That Misidentify Themselves to Circumvent Access Restrictions on Password-Protected Websites Violate the “Without Authorization” Prong of the CFAA.....	18
1. Access Credentials That a Bot Obtains by Misidentification Are Not “Authorization”	18
2. Bots That Misidentify Themselves to Gain Access to Protected Websites Without Authorization Harm Publishers and Other Website Operators.....	19

III.	FINDING CFAA LIABILITY UNDER THESE CIRCUMSTANCES WILL NOT RUN AFOUL OF THE FIRST AMENDMENT	23
IV.	CONCLUSION	28

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Associated Press v. Meltwater U.S. Holdings, Inc.</i> , 931 F. Supp. 2d 537 (S.D.N.Y. 2013).....	5, 28
<i>Branzburg v. Hayes</i> , 408 U.S. 665 (1972).....	23
<i>City of Fullerton v. Friends for Fullerton’s Future</i> , No. 30-2019-01107063-CU-NP-CJC (Orange Cnty. Sup. Ct. filed Nov. 5, 2019)	25
<i>Daily Herald Co. v. Munro</i> , 838 F.2d 380 (9th Cir. 1988).....	24
<i>Fla. Star v. B.J.F.</i> , 491 U.S. 524 (1989).....	24
<i>Nicholas v. Bratton</i> , 376 F. Supp. 3d 232 (S.D.N.Y. 2019).....	24
<i>Sandvig v. Sessions</i> , 315 F. Supp. 3d 1 (D.D.C. 2018)	26
<i>Smith v. Daily Mail Publ’g Co.</i> , 443 U.S. 97 (1979).....	23
<i>Van Buren v. United States</i> , 593 U.S. 374 (2021).....	26
Statutes	
18 U.S.C. § 1030(a).....	4
Cal. Penal Code § 502 (West)	2, 4, 25
Cal. Penal Code § 502(c) (West)	4

Computer Fraud and Abuse Act, 18 U.S.C. § 1030	<i>passim</i>
Computer Fraud and Abuse Act, Pub. L. No. 103–322, 108 Stat. 1796 (1994).....	4
Crimes and Offenses-Computers-Violations, 1987 Cal. Legis. Serv. 1499 (West).....	4
Other Authorities	
<i>Cloudflare Bot Management</i> , Cloudflare (last visited Apr. 29, 2026), https://www.cloudflare.com/application-services/products/bot-management/	10
<i>The Cost of a Journalism Story</i> , My News Desk (Sep. 6, 2018), https://www.mynewsdesk.com/en/blog/the-cost-of-a-journalism-story/	8
<i>Does AI Take Your Data? AI and Data Privacy</i> , National Cybersecurity Alliance (Mar. 31, 2025), https://www.staysafeonline.org/articles/does-ai-take-your-data-ai-and-data-privacy	21
Gabriel Dorosz, <i>News Publisher Diversification and the Rise of “Other” Revenue</i> , INMA (Mar. 16, 2026), https://www.inma.org/blogs/advertising-initiative/post.cfm/news-publisher-diversification-and-the-rise-of-other-revenue	6
George Montagu and Lamberto Lambertini, <i>Dynamic, Cheap, and “Shocking”: The Evolution of Paywalls, Pricing, and Trials in the News Industry</i> , FT Strategies (last visited Apr. 29, 2026), https://www.ftstrategies.com/en-gb/insights/dynamic-cheap-and-shocking-the-evolution-of-paywalls-pricing-and-trials-in-the-news-industry	11
<i>Guest Blog: Paywalls - What You Can Learn from Wired, Bild, The Athletic and Co.</i> , PPA (Apr. 14, 2020), https://ppa.co.uk/guest-blog-paywalls-what-you-can-learn-from-wired-bild-the-athletic-and-co	11

<i>In Graphic Detail: New Data Shows Publishers Face Growing AI Bot, Third-Party Scraper Activity</i> , DIGIDAY (Apr. 13, 2026), https://digiday.com/media/in-graphic-detail-new-data-shows-publishers-face-growing-ai-bot-third-party-scraper-activity/	18
Lola Murti, <i>AI and Bots Have Officially Taken Over the Internet, Report Finds</i> , CNBC (Mar. 26, 2026, at 9:00 ET), https://www.cnbc.com/2026/03/26/ai-bots-humans-internet.html	6
Malika Mukhanova and Xiao Yang, <i>News Publishers Leverage Paywalls to Increase Revenue, Engagement</i> , INMA (Mar. 12, 2025), https://www.inma.org/blogs/conference/post.cfm/news-publishers-leverage-paywalls-to-increase-revenue-engagement	11
<i>Media Industry Continues Reshaping Workforce in 2025 Amid Digital Shift</i> , InsideRadio (Dec. 31, 2025), https://www.insideradio.com/free/media-industry-continues-reshaping-workforce-in-2025-amid-digital-shift/article_403564f7-08ce-45a1-9366-a47923cd2c09.html	5
Melissa De Witte, <i>Stanford Scholars Are Helping Journalists Do Investigative Journalism Through Data</i> , Stanford Rep. (Oct. 15, 2018), https://news.stanford.edu/stories/2018/10/helping-journalists-use-data-investigative-reporting	8
Peter Osnos, <i>These Journalists Spent Two Years and \$750,000 Covering One Story</i> , The Atlantic (Oct. 2, 2013), https://www.theatlantic.com/national/archive/2013/10/the-se-journalists-spent-two-years-and-750-000-covering-one-story/280151/	8

Sherman Smith *et al.*, *Police Stage 'Chilling' Raid on Marion County Newspaper, Seizing Computers, Records and Cellphones*, Kansas Reflector (Aug. 11, 2023, at 17:15 CT), <https://kansasreflector.com/2023/08/11/police-stage-chilling-raid-on-marion-county-newspaper-seizing-computers-records-and-cellphones/> 25

Thomas Claburn, *Claude Code Source Leak Reveals How Much Info Anthropic Can Hoover up About You and Your System*, The Register (Apr. 1, 2026), https://www.theregister.com/2026/04/01/claude_code_source_leak_privacy_nightmare/..... 21

U.S. Const. amend. I 23, 24, 25, 26, 27

STATEMENT OF INTEREST OF *AMICUS CURIAE*

News/Media Alliance (“NMA”) is a nonprofit organization representing over 2,200 publishers in the United States. As the leading voice for news, magazine, and digital publishers, its members range from the largest news and magazine publishers in the country to hyperlocal publications, and from digital-only outlets to papers that have printed since before the nation’s founding. NMA’s membership accounts for nearly 90 percent of the daily newspaper circulation in the United States, and over 500 magazine and digital-only brands. NMA advocates for laws and policies that let high-quality journalism thrive in the digital age. This brief seeks to highlight the concerns of news organizations whose business models and viability in the online environment rely on monetizing their content through their websites, which requires the ability to control access to their content online. NMA writes to address a critical, but narrow, question: whether a person or company (in this case, Perplexity) violates the “without authorization” prong of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, and the “knowingly accesses” and/or “without permission” prongs of the California Comprehensive Computer Data Access and Fraud Act (“CDAFA”), Cal.

Penal Code § 502 (West), when it deploys automated crawlers, “bots,” or a third-party AI “agent” to access password-protected areas of a website or computer system, where the website owner specifically and explicitly prohibits such access but a user supplies their login credentials. The answer to that question is Yes.

This brief is submitted with the consent of all parties.

RULE 29(a)(4)(E) CERTIFICATION

No person or entity other than counsel for NMA authored or contributed funds intended for the preparation or submission of the instant brief.

s/ Michael S. Elkin

Michael S. Elkin

Attorney for Amicus Curiae

SUMMARY OF ARGUMENT

Amicus News/Media Alliance (“NMA”) writes, as the leading organization representing news, magazine, and digital media publishers in the United States and internationally, to support Amazon in opposing Perplexity’s unauthorized access of information from protected areas of Amazon’s website and to urge the Court to uphold the district court’s preliminary injunction against Perplexity. Perplexity has deployed its AI agent to access Amazon’s password-protected system “without authorization,” as required by the Computer Fraud and Abuse Act (“CFAA”). But the putative “permission” Perplexity claims to receive when Amazon users log into their Amazon accounts does not amount to valid authorization for *Perplexity* to enter *Amazon’s* computer systems, and even if it did, Amazon’s express repudiation of authorization and technical methods to block Perplexity’s bots are sufficient to revoke it.

And the type of information that Perplexity concededly obtained from Amazon’s protected servers, including account details, shopping history, payment information, shipping addresses, and other personal and financial data that helps operationalize Amazon’s website, 2-SR-330, is accessible only to logged-in Amazon users and so is squarely protected

by the CFAA. Perplexity’s conduct, as described by Perplexity itself, constitutes a clear-cut violation of the CFAA.¹

Perplexity’s arguments for how it believes the CFAA should be interpreted sweep so broadly that if the Court were to adopt them it would gut the statute, depriving not only Amazon but other companies—indeed, even entire industries—of critical protections from harmful, unauthorized incursions into their protected computer systems.² A ruling that the CFAA does not apply when unauthorized third-party bots or agents attempt to access password- or paywall-protected information, despite a website owner’s direct prohibition, would undermine the ability

¹ NMA’s comments about the CFAA apply with equal force to its state-law analog, the CDAFA. The CDAFA is broader than the CFAA in important ways: primarily, while the CFAA requires *unauthorized* access to a protected computer system, 18 U.S.C. § 1030(a), the CDAFA provides a remedy when a bad actor *knowingly* engages in various access-related activities that result in alteration, damage, deletion, destruction, or other disruption to the system. *See* Cal. Penal Code § 502(c) (West) (emphasis added).

² While Perplexity mischaracterizes the CFAA and the CDAFA as “criminal anti-hacking statutes,” 1-SER-90, the CFAA has provided a civil cause of action for more than three decades, and the CDAFA has provided a civil cause of action since its inception in 1987. Computer Fraud and Abuse Act, Pub. L. No. 103–322, § 290001, 108 Stat. 1796, 2097–99 (1994); Crimes and Offenses—Computers—Violations, 1987 Cal. Legis. Serv. 1499 (West).

of news publishers, as well as a host of other businesses, to generate the revenues essential to thrive in the digital economy.

In applying the statute and weighing the public interest, the Court should avoid harming the efforts of news organizations to sustainably produce and distribute the news online, an “essential function of democracy” that fulfills a “strong public interest in preserving this democratic, instantaneous, and efficient access to information.” *See Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 553 (S.D.N.Y. 2013). Perplexity’s proposed interpretation of the CFAA would allow commercial actors to reap where they have not sown, by creating a gap in the protections that news publishers rely on to maintain viability.³ News organizations already navigate strong headwinds, and the unprecedented rise of bot scraping and unauthorized reuse of publisher content for commercial AI purposes adds to these challenges, with recent reports showing that bots have surpassed human internet

³ *See Media Industry Continues Reshaping Workforce in 2025 Amid Digital Shift*, InsideRadio (Dec. 31, 2025), https://www.insideradio.com/free/media-industry-continues-reshaping-workforce-in-2025-amid-digital-shift/article_403564f7-08ce-45a1-9366-a47923cd2c09.html.

traffic.⁴ Publishers monetizing their content through websites or apps must have the ability to control access to their content, including through password protections or paywalls, and to generate revenues through digital advertising, subscriptions, or other strategies like partnerships or licensing.⁵ Moreover, with advertisers increasingly focused on being able to confidently identify who they are reaching, how audiences engage, and what outcomes media delivers, publishers must be able to demonstrate that they have direct relationships with high-value, human users to differentiate and command maximum value from advertisers.⁶ News publishers' ability to have a sustainable business model in the online environment depends on their ability to unequivocally control access to content—including distinguishing between human users and bots when

⁴ Lola Murti, *AI and Bots Have Officially Taken Over the Internet, Report Finds*, CNBC (Mar. 26, 2026, at 9:00 ET), <https://www.cnbc.com/2026/03/26/ai-bots-humans-internet.html>.

⁵ According to the International News Media Association (“INMA”), the publishers “posting the strongest results” have “[i]nvested in premium, direct-sold advertising. First-party data, contextual targeting tools, premium formats, video inventory.” Gabriel Dorosz, *News Publisher Diversification and the Rise of “Other” Revenue*, INMA (Mar. 16, 2026), <https://www.inma.org/blogs/advertising-initiative/post.cfm/news-publisher-diversification-and-the-rise-of-other-revenue>.

⁶ *See supra* note 5.

deciding whether to grant such access. Among the most important tools are electronic registration walls and paywalls that permit authorized access to publishers' content, while restricting the access of unauthorized persons, including AI agents, crawlers, and fetchers.

A ruling that Perplexity's access was "authorized" even after Amazon expressly prohibited Perplexity from accessing the relevant password-protected portions of Amazon's website would severely weaken the CFAA and cripple website operators' ability to control access to their websites against bad actors (including those who engage in unauthorized scraping and the theft of private consumer data). Similarly, a ruling that permitted Perplexity to circumvent technical barriers to gain access against Amazon's express prohibition would harm news publishers by depriving them of a critical tool to identify and deal with unauthorized bots, including so-called agentic bots that operate autonomously and often, from the point of view of a human user, unpredictably.

This Court should uphold the district court's narrow preliminary injunction.

ARGUMENT

I. NEWS ORGANIZATIONS RELY ON THE ABILITY TO EFFECTIVELY MANAGE ACCESS TO THEIR CONTENT TO BE ECONOMICALLY VIABLE IN AN ONLINE ENVIRONMENT

Faced with significant headwinds, news publishers must maintain viability by developing ways to monetize their content through their websites. Creating high-quality journalism is an expensive undertaking: publishers employ professional journalists to produce investigative reporting, and lifestyle, business, and opinion coverage, among other types of content, while delivering an accurate stream of breaking news covering local, national, and global events.⁷ They invest in editorial,

⁷ See, e.g., Melissa De Witte, *Stanford Scholars Are Helping Journalists Do Investigative Journalism Through Data*, Stanford Rep. (Oct. 15, 2018), <https://news.stanford.edu/stories/2018/10/helping-journalists-use-data-investigative-reporting> (“[I]t can cost newsrooms up to \$300,000 and six months of a reporter’s time to do a deep dive into public interest issues like crime and corruption. In one case, it cost a newsroom \$487,000 to produce an investigative series on local police shootings.”) (emphasis omitted); *The Cost of a Journalism Story*, My News Desk (Sep. 6, 2018), <https://www.mynewsdesk.com/en/blog/the-cost-of-a-journalism-story/> (estimating the cost of a detailed or investigative news story to be \$400 to \$12,000, a general news story to be \$100 to \$4,500, and filler story to be \$50 to \$300); Peter Osnos, *These Journalists Spent Two Years and \$750,000 Covering One Story*, The Atlantic (Oct. 2, 2013), <https://www.theatlantic.com/national/archive/2013/10/these-journalists-spent-two-years-and-750-000-covering-one-story/280151/> (“We conservatively estimate the cost of this coverage [of the dangers of

operational, security, and legal support for their reporters. Publishers must find ways to sustain their significant investments if they are to continue serving these essential functions.

In today's predominantly digital media environment, the largest sources of news publishers' revenues are subscriptions and advertising. In addition, publishers may earn revenues by entering into content distribution licenses, including deals with syndicators or platform aggregators like Apple News. Publishers may also derive revenue from digital affiliate link arrangements, which work only when human consumers follow the links and purchase featured products and services. Effective access controls, including technological measures like account registration requirements and paywalls, are critically important to all these models. To effectively monetize their news content and generate critical revenue by these means, publishers must be able to exercise meaningful control over access to their content online and the means of such access.

acetaminophen] at \$750,000; it could be more. This covers the reporters, news applications and web developers, editors, video production, social media and PR, travel, legal review, half of the public opinion poll etc.”).

While the present litigation is directed at protecting access to secure components of the e-commerce facilities of Amazon’s marketplace website, the same means of control power the incentives for news publishers to invest, produce, and distribute valuable content that is unavailable to the general public without authorization. Publishers protect access to and use of their content in a variety of ways—such as robots.txt files,⁸ terms of service, third-party bot blocking services like Cloudflare,⁹ and legal enforcement efforts—but one of the most important means of access control is through “walling” practices that permit access to content for authorized users and paying subscribers, while restricting the access of unauthorized actors. News publishers often use a registration wall that requires visitors to register, provide identifying information, and create a personal account before they can access content. This step is critical to build and track consumer

⁸ A “robots.txt” file is used to implement the Robots Exclusion Protocol, a standard by which websites can instruct bots which portions of the website they are allowed to access.

⁹ Cloudflare’s Bot Management service analyzes online behavior and anomalies in network traffic to detect and manage “good and bad bots.” See *Cloudflare Bot Management*, Cloudflare (last visited Apr. 29, 2026), <https://www.cloudflare.com/application-services/products/bot-management/>.

engagement; to support online advertising, affiliate marketing, and other revenue opportunities; and as a key step in converting users into paying subscribers. A registration wall may, or may not, also require payment in order to access some content, such as exclusive or premium content. These paywalls can be fine-tuned to customize offers to incentivize users to subscribe, and also to support tracking advertising exposure and assessing ad effectiveness, among other things.¹⁰ Each of these activities

¹⁰ See, e.g., George Montagu and Lamberto Lambertini, *Dynamic, Cheap, and “Shocking”: The Evolution of Paywalls, Pricing, and Trials in the News Industry*, FT Strategies (last visited Apr. 29, 2026), <https://www.ftstrategies.com/en-gb/insights/dynamic-cheap-and-shocking-the-evolution-of-paywalls-pricing-and-trials-in-the-news-industry> (explaining that reader registration allows publishers to improve “brand awareness (via free newsletters, podcasts, events, and much more) [and] serve[s] specific needs, especially in moments of heightened news cycles, and, of course, the pricing of [] product packages”); *Guest Blog: Paywalls – What You Can Learn from Wired, Bild, The Athletic and Co.*, PPA (Apr. 14, 2020), <https://ppa.co.uk/guest-blog-paywalls-what-you-can-learn-from-wired-bild-the-athletic-and-co> (reporting that after *Wired* magazine introduced its paywall it experienced a 300% increase in digital subscribers); Malika Mukhanova and Xiao Yang, *News Publishers Leverage Paywalls to Increase Revenue, Engagement*, INMA (Mar. 12, 2025), <https://www.inma.org/blogs/conference/post.cfm/news-publishers-leverage-paywalls-to-increase-revenue-engagement> (reporting that that after introducing a registration process, *El Mundo*’s subscription conversion increased by 60.4% and revenue grew by 50.7%, and that the *Philadelphia Inquirer* used a registration system “to evaluate user behavior and content value, gating or unlocking content based on the likelihood of conversion or ad revenue potential. Premium content,

assumes the ability to distinguish between a human user navigating the site, as opposed to a bot.

Perplexity’s flawed interpretation of the CFAA would strip publishers of a crucial tool for controlling access by means that distinguish human traffic from bot traffic. It would also hinder development of secure technical mechanisms that help facilitate contractual arrangements between publishers and deployers of bots. This Court should reject that interpretation, which is contrary to law and the CFAA’s underlying public-policy goals.

II. ACCESS IN CONTRAVENTION OF PROHIBITIONS AGAINST AI AGENTS OR “BOTS” VIOLATES THE CFAA

A. Perplexity’s Conduct Violates the CFAA Because Perplexity Itself Accesses a Protected Website but Lacks Authorization to Do So

Perplexity developed and makes available to the public a web browser called “Comet.” Comet users, like users of other browsers, can access internet sites (such as Amazon’s eponymous e-commerce site). Once there, a Comet user—unlike users of other browsers—can launch Perplexity’s AI agent and give it instructions to perform website-related

including investigative reports and expert analysis, is often gated to reinforce the value of a subscription”).

tasks on the user’s behalf. As Perplexity explains, the Perplexity AI agent engages in “data collection” by “logging and sending to [Perplexity] data the users receive from Amazon” while they are logged in. 1-SER-99 (alterations in original). This includes “view[ing] and analyz[ing] the data sent by Amazon to the user’s computer” while the agent is “engaged” in activity that requires a user to be logged in to the website—such as “mak[ing] a purchase on Amazon.com.” 1-SER-100 (emphasis omitted). In the other direction, when the AI agent “takes actions,” those actions “are communicated by the user’s computer to Amazon’s servers.” 1-SER-100.

Although Perplexity tries to characterize its AI agent as simply a neutral, user-directed “tool” that authorized persons can deploy as a matter of efficiency or convenience, Perplexity’s papers make clear that it is Perplexity that is operating the bot and accessing Amazon’s systems: the bot runs on *Perplexity’s* servers, and it obtains information from Amazon’s servers and returns it *to Perplexity*, for *Perplexity’s* potential use, all in direct violation of Amazon’s express commands to stop, as well as Amazon’s attempts to block *Perplexity’s* bot access by technical means. This conduct violated the CFAA.

Beyond the instant case, a rule holding that unauthorized access by bots falls outside the ambit of the CFAA would cripple publishers' ability to control access to their websites, and consequently cripple their ability to earn revenues to support the creation of original content.

In addition to providing news publishers with a means of preventing their content from being taken without permission, controlling access to nonpublic areas of a website or computer system enables publishers to monetize their content. As described above, key revenue models like advertising and paid subscriptions depend on human users—not automated bots or AI agents—navigating registration or paywall access gates to and through the site.¹¹ Unauthorized third parties should not be able to access protected sites and obtain information (whether private financial information, paywall-protected news content, or other protected content) under the pretext that “permission” from an authorized user is the legal equivalent of *actual authorization* from the website's owner. Basic tenets of contract and agency law preclude that

¹¹ Similarly, licenses can be undermined and their value sapped when access controls are unenforceable.

result, and a rule that permitted it would wreak havoc with the online-publishing ecosystem.

B. The Type of Information Perplexity Obtained from Amazon’s Protected Website Implicates the CFAA

NMA does not dispute that if Perplexity accessed only the publicly available portions of Amazon’s website—those portions viewable without logging in—that would not, in itself, violate the CFAA. But Perplexity is accused of accessing Amazon’s password-protected systems without authorization to obtain highly sensitive information, including information allowing Perplexity to further leverage its unauthorized access to operationalize Amazon’s website and make it perform actions that members of the general public, lacking such access, would be unable to perform. As the district court correctly explained, Perplexity’s AI agent “obtain[s] information as to the user’s private Amazon account information ... [which] is transmitted to Perplexity’s servers for the purpose of conducting said user’s requested tasks.” PI Order at 3.¹²

¹² Perplexity concedes that the information at issue is not limited to publicly available information. *See* Perplexity Br. at 16–17.

C. Perplexity’s Continued Access After Amazon Expressly Prohibited It from Accessing Password-Protected Areas of the Website Violated the CFAA

Even if the Court were to credit Perplexity’s theory that it was authorized to access protected areas of Amazon’s website when it received “permission” from an Amazon user, any putative authorization would not have survived Amazon’s express, unequivocal, and repeated revocation of authorization. A ruling that Perplexity’s access was authorized even *after* Amazon expressly prohibited Perplexity from accessing password-protected areas of the website would be contrary to the CFAA.

NMA agrees with Amazon that ordinary users of the website cannot “pass along” their access rights to a bot, or to a third party more generally, once the website owner has expressly informed the third party that this activity is prohibited. As a general matter, the right to “authorize” site access belongs to a site owner, not a user. At a minimum, whatever permission such users or subscribers may have granted to a third party (including to assist them or act on their behalf) could not survive express withdrawal of authorization. For example, website owners often send cease-and-desist letters to technology companies to put them on notice

that they are engaging in unauthorized behavior. It is not possible for a user to override an express communication like that and give the technology company access by extending it “permission.” Here, once Amazon had informed Perplexity that it was not authorized to access the password-protected areas of its website using Perplexity’s AI agent, any subsequent access to the website was “without authorization” for CFAA purposes.¹³

In short, once authorization to visit protected areas of the website is expressly rescinded, it is an enforceable bar on future access to protected information. Where a website operator (like Amazon, news publishers, or any other whose content is protected by access controls) expressly informs a bot operator (like Perplexity or any other operator) that it is *not* authorized to access content on paywall-protected or

¹³ This common-sense interpretation of the CFAA is not, contrary to Perplexity’s strained argument, likely to stifle innovation. A user wishing to give a third-party bot like Perplexity’s AI agent access to a website may do so if, and only if, the website operator has reached an agreement with the bot deployer to facilitate that preference. An interpretation of the CFAA that allows the bot deployer to effectively cut the website owner out of the equation will prevent these technologies from developing securely and fairly.

otherwise protected areas of their websites, the bot cannot continue to do so without violating the CFAA.

D. Bots That Misidentify Themselves to Circumvent Access Restrictions on Password-Protected Websites Violate the “Without Authorization” Prong of the CFAA

1. Access Credentials That a Bot Obtains by Misidentification Are Not “Authorization”

Because effective authorization depends on accurate identification, a bot that misidentifies itself to obtain access violates at least the “without authorization” prong of the CFAA, in circumstances where the prohibition on access has been communicated. A contrary holding would effectively legitimize, indeed encourage, fraud and wrongdoing. At a minimum, this Court should affirm that when access has been gained to a protected website by misrepresenting the nature of a bot or AI agent after an access prohibition has been communicated to the bot operator, such access cannot legitimately be considered authorized.

In today’s environment, where AI bot activity has risen 300 percent since 2025,¹⁴ companies are sending bot traffic to publishers’ sites under

¹⁴ Sara Guaglione, *In Graphic Detail: New Data Shows Publishers Face Growing AI Bot, Third-Party Scraper Activity*, DIGIDAY (Apr. 13, 2026),

false pretenses, misrepresenting or concealing the nature and identities of these bots to gain access that the site owners expressly prohibit. This type of misrepresentation includes providing false information to obtain an account or to bypass the need to get an account. It can also include other efforts to mask the identity of the bot to circumvent technical measures or deceive the website owner into believing it is a human. A bot that misrepresents itself as an authorized entity in order to bypass a technological access restriction (such as a subscription wall, paywall, or password requirement) that would otherwise apply to it, or in contravention of an express revocation of authorization, so as to obtain credentials that allow it to access a protected website, cannot be said to have “authorization” for purposes of the CFAA.

2. Bots That Misidentify Themselves to Gain Access to Protected Websites Without Authorization Harm Publishers and Other Website Operators

Bots that misidentify themselves or mask their nature in order to gain access to protected content are a serious problem for news publishers, who—like virtually all website owners, including Amazon—

<https://digiday.com/media/in-graphic-detail-new-data-shows-publishers-face-growing-ai-bot-third-party-scraping-activity/>.

fight a constant battle to ward off malicious bots that act without authorization. Bots that disguise their identity to circumvent technical barriers and engage in prohibited activity are a serious drain on resources: they add bandwidth costs, frequently degrade service, and force website owners to take extraordinary measures to identify, analyze, block, or mitigate the harm that they cause. For example, many such bots (including those used by Perplexity) routinely circumvent paywalls to scrape content in bulk and without permission, in violation of express prohibitions. This conduct harms publishers' rights and ability to protect their content and—as in Amazon's case—ensure the integrity of their websites. And by misidentifying themselves, such bots also make it difficult or impossible for publishers to take legitimate actions to mitigate the harms caused.

Bots that misrepresent their identity to gain access to protected information also disrupt publishers' relationships with their readers and prevent publishers from creating meaningful, engaging experiences that bring people back to websites and encourage subscriptions. And when malicious, misidentified bots bypass website features that were designed and implemented with human users in mind, they also have the potential

to dilute and disrupt advertising markets that depend on accurate information about conversion, clicks, and views. Permitting unfettered access by unidentified bots could disrupt online markets or undermine security by enabling automated behavior, including industrial-scale or high-bandwidth activity, that the website was not designed to handle. Further, even if a bot operator (like Perplexity here) claims it will obtain only specific information that the user would be unlikely to object to, an intruder’s purported intent is irrelevant to the “gate up / gates down” inquiry, especially when—as here—there appears to be no principle that limits its collection or use of the information it obtains. Time and again, AI companies have been caught copying and stockpiling information that they acquire from users, “exercis[ing] far more control over people’s computers than even the most clear-eyed reader of contractual terms might suspect ... and retain[ing] lots of [user] data[.]”¹⁵

¹⁵ See, e.g., Thomas Claburn, *Claude Code Source Leak Reveals How Much Info Anthropic Can Hoover up About You and Your System*, The Register (Apr. 1, 2026), https://www.theregister.com/2026/04/01/claude_code_source_leak_privacy_nightmare/; see also, e.g., *Does AI Take Your Data? AI and Data Privacy*, National Cybersecurity Alliance (Mar. 31, 2025), <https://www.staysafeonline.org/articles/does-ai-take-your-data-ai-and-data-privacy> (“AI models process and store data differently than traditional software. Public AI platforms often retain input data for

A core purpose of the CFAA is to provide online website operators effective means to counter computer hacking. Hacking, however, is not limited to the circumvention of access barriers by technological means: it includes obtaining unauthorized access to a computer through misrepresentation, camouflage, or subterfuge. When a website owner gives a clear “gates down” signal to a class of putative authorization-seekers, such as malicious bots or AI agents, misrepresentation by such a bot in order to gain or continue unauthorized access violates the CFAA. In other words, misrepresentation is “gate-evading” conduct at the point of access and, as such, prohibited by the CFAA. A contrary rule that the CFAA is *not* violated when a bot intentionally misrepresents its identity to obtain access would open the door to fraudsters and bad actors, and deprive website owners of critical means of protecting their websites, including against entities that would use their access to compete unfairly.

For these and other reasons, Perplexity violated the “without authorization” prong of the CFAA when it disguised its AI agent as an ordinary browser, so that its activity would be indistinguishable from the

training purposes, meaning that anything you share could be used to refine future responses—or worse, inadvertently exposed to other users.”).

activity of an ordinary human user—including by pushing an update that evaded detection once Amazon devised a means of detecting the AI agent. Activity such as this, which circumvents access controls by obtaining credentials under false pretenses, clearly does not equate to genuine authorization under the CFAA. Accordingly, this Court should adopt a rule that when a bot (including nonhuman, automated, or autonomous systems like Perplexity’s AI agent) misidentifies or fails to accurately identify itself at the point of access control, in direct contravention of an express identification requirement, it does not have *authorized* access to the website.

III. FINDING CFAA LIABILITY UNDER THESE CIRCUMSTANCES WILL NOT RUN AFOUL OF THE FIRST AMENDMENT

First Amendment concerns are of course paramount to NMA and its members. Journalists unquestionably have a First Amendment right to engage in traditional news-gathering activities—and that includes reviewing and obtaining publicly available information, including by scraping websites. *See Branzburg v. Hayes*, 408 U.S. 665, 681 (1972) (“[W]ithout some protection for seeking out the news, freedom of the press could be eviscerated.”); *Smith v. Daily Mail Publ’g Co.*, 443 U.S. 97,

103–04 (1979) (holding that reporters were protected by the Constitution when they “relied upon routine newspaper reporting techniques to ascertain the identity of the alleged assailant”); *Fla. Star v. B.J.F.*, 491 U.S. 524, 538–39 (1989) (holding that the First Amendment shielded newspaper from liability for reporting name of sexual-offense victim that appeared in publicly released police report, notwithstanding statute making it unlawful to do so, because “[r]eliance on a news release is a paradigmatically routine newspaper reporting technique”) (citation modified); *Nicholas v. Bratton*, 376 F. Supp. 3d 232, 279 (S.D.N.Y. 2019) (“[E]ntrenched in Supreme Court case law is the principle that the First Amendment’s protections for free speech include a constitutionally protected right to gather news.”); *Daily Herald Co. v. Munro*, 838 F.2d 380, 384 (9th Cir. 1988) (explaining that “the First Amendment protects the media’s right to gather news” and that newspaper could not be held liable for conducting exit polling in violation of state statute: exit polling was “speech that is protected, on several levels, by the First Amendment”).

NMA agrees with *amici* the American Civil Liberties Union and the Knight First Amendment Institute that the CFAA has at times in the

past been applied too expansively, including in ways that conflict with legitimate First Amendment activity. *See* Dkt. No. 30 at 13–18. First Amendment concerns have arisen when the CFAA and analogous state laws were interpreted in ways that would criminalize accessing publicly available information *without* circumventing log-in screens or paywalls. For example, in 2019, the city of Fullerton, California sued local bloggers, accusing them of CFAA and CDAFA violations for accessing publicly available files that the town had intended to keep confidential. *City of Fullerton v. Friends for Fullerton’s Future*, No. 30-2019-01107063-CU-NP-CJC (Orange Cnty. Sup. Ct. filed Nov. 5, 2019); *City of Fullerton v. Friends for Fullerton’s Future*, Reporters Committee for Freedom of the Press (last visited Apr. 29, 2026). In 2023, Marion County police raided the newsroom of a weekly newspaper and the home of its owner under the claim of enforcing a computer crime law, after the newspaper received a screenshot of a local businesswoman’s driving record from a confidential source; the police seized computers, cellphones, and documents. *See* Sherman Smith *et al.*, *Police Stage ‘Chilling’ Raid on Marion County Newspaper, Seizing Computers, Records and Cellphones*, Kansas Reflector (Aug. 11, 2023, at 17:15 CT),

<https://kansasreflector.com/2023/08/11/police-stage-chilling-raid-on-marion-county-newspaper-seizing-computers-records-and-cellphones/>.

The narrow dispute before this Court does not implicate those important First Amendment and policy interests. Instead, it involves a company’s attempt to access protected areas of a website for commercial purposes, after the website operator demanded that the company cease access and despite the website operator’s technical efforts to restrict access. This is unauthorized access squarely within the scope of the CFAA.¹⁶

News gathering—which is a necessary precursor to actually engaging in speech—dovetails two core First Amendment principles: “the freedom of speech” and “the freedom ... of the press.” U.S. Const., amend. I; see *Sandvig v. Sessions*, 315 F. Supp. 3d 1, 15–16 (D.D.C. 2018) (“The

¹⁶ Nor is this a case in which a website owner is attempting to limit otherwise authorized access to those “permitted” in terms of service. Courts have rightly been skeptical of such attempts, recognizing the risk that “criminaliz[ing] every violation of a computer-use policy” could make “millions of otherwise law-abiding citizens ... criminals.” *Van Buren v. United States*, 593 U.S. 374, 394 (2021). But here, Perplexity is using its AI agent to circumvent Amazon’s *login page* and access *nonpublic* portions of Amazon’s website by pretending to be a human user. This is unauthorized access at the front gate, pure and simple.

Supreme Court has made a number of recent statements that give full First Amendment application to the gathering and creation of information. Additionally, six courts of appeals have found that individuals have a First Amendment right to record at least some matters of public interest, in order to preserve and disseminate ideas.”).

But here, Perplexity does not access protected content to gather information that can be used to craft news stories, or anything like it. Far from acting in the public interest, Perplexity seeks to access nonpublic portions of Amazon’s website because it wishes to use the information stored there to engage in commercial transactions. The First Amendment provides neither a defense to such illicit conduct, nor a justification for removing large swaths of wrongful conduct from the CFAA’s important protections.

Nor did Perplexity, in opposing the preliminary injunction, even attempt to articulate a public interest in its *access* to the information at issue. Instead, it hung its argument on a straw man: that the District Court’s narrow preliminary injunction somehow threatens the very existence of agentic AI technology by “stifling consumer choice, fair competition, and innovation.” 1-SER-111; *see* 1-ER-6 (discussing

Perplexity’s argument that a preliminary injunction “would be contrary to the public’s interest in consumer choice and innovation”).

This Court should not interpret the CFAA in a way that privileges Perplexity’s theory of “public interest” over the important public interests served by other industries and organizations—including the public’s strong interest in a robust, viable press, distributed to readers online. As the *Meltwater* court explained, the public interest disfavors commercial conduct that “injures [a news publisher’s] ability to perform this essential function of democracy.” *See Meltwater*, 931 F. Supp. 2d at 553 (analyzing public interest in the context of copyright law). So too here.

IV. CONCLUSION

Perplexity’s self-described conduct in this case violates the “without authorization” prong of the CFAA; this Court should so hold and affirm the district court’s Preliminary Injunction Order.

Dated: April 29, 2026

Respectfully submitted,

s/ Michael S. Elkin

Michael S. Elkin
Sean R. Anderson
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166
(212) 294-6700
melkin@winston.com
sranderson@winston.com

Jennifer A. Golinveaux
Thomas J. Kearney
WINSTON & STRAWN LLP
101 California Street Floor 21
San Francisco, CA 94111
(415) 591-1000
jgolinveaux@winston.com
tkearney@winston.com

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: <http://www.ca9.uscourts.gov/forms/form08instructions.pdf>

9th Cir. Case Number: 26-1444

I am the attorney or self-represented party.

This brief contains 5,297 words, including zero words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief (*select only one*):

complies with the word limit of Cir. R. 32-1.

is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

complies with the longer length limit permitted by Cir. R. 32-2(b) because (*select only one*):

it is a joint brief submitted by separately represented parties.

a party or parties are filing a single brief in response to multiple briefs.

a party or parties are filing a single brief in response to a longer joint brief.

complies with the length limit designated by court order dated _____.

is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature /s/ Michael S. Elkin **Date: April 29, 2026**
(use "s/[typed name]" to sign electronically-filed documents)